TCA Translation

PP

REPUBLIC OF FRANCE

Publication No.: 2,697,653
(Use only for reprint orders)

NATIONAL INSTITUTE OF
INDUSTRIAL PROPERTY
PARIS

National registration No.: 92 13239

Int. Cls.: G 07 C 15/00

APPLICATION FOR INVENTION PATENT A1

Application date: 11/4/92

Priority: /no entry/

Applicant(s): Corporation named INFO TELECOM - FR and mixed economy corporation called: LA FRANCAISE DES JEUX - FR.

Inventor(s): Reibel, Jean-Michel, Simon, Pierre-Luc, Bigonneau, Eric, and Bouedec, Jean-Etienne.

Date of publication of the application: 5/6/94 Bulletin 94/18.

List of documents cited in the preliminary research report: See the end of this brochure.

References to other related national documents: /no entry/

Principal(s): /no entry/

Mandatary: Bureau D.A. Casalonga - Josse.

Electronic system implementing a game of chance.

A portable unit (11) has memory circuits that can store at least one set of reference data, and comparison media that can compare said reference data to game data introduced by the player through a communication interface, whereby one of these two data sets is a randomly generated value. Gain information depending at least on the result of said comparison is stored in the memory, and unit encryption media, in response to predetermined payment request information (PRI) received, can establish a first encrypted gain value based on said gain information. An external station (12) outside the unit (11) contains an input/output interface (17), which communicates with the interface of the unit, and processors (16) which, in the presence of a request for payment by the player, can read said gain information contained in the memory of the unit. System encryption media (19), analog to the unit encryption media, establish a second encrypted gain value based on said gain information being read. Pay-off to the player depends on the matching of the two encrypted gain values.
/In margin:/ FF 2,697,653 - A1 /Drawing/

Electronic system implementing a game of chance.

The present invention relates to an electronic system implementing a game of chance.

Currently, there are various known games of chance allowing a player to win money after paying a starting wager. Thus, for example, in the "loto" /lottery/ game (registered trademark), the player marks a series of numbers on a ticket which must be validated with a specialized agency, paying a price corresponding to the starting wager. Subsequently, a supervised drawing of lots takes place at a chosen venue, and the players holding a winning ticket may withdraw their gain from a payor entity.

Compared to these classic games, which require the use of paper and drawings of lots on predetermined dates, valid for all players, the invention provides a radically different concept of a system implementing a game of chance.

It is an object of the invention to provide an autonomous, portable unit allowing a player to make one or several wagers, the success or failure of which determine a score, or gain level, according to predetermined game rules. Said unit also constitutes the transaction element for the payment of the winnings, and comprises all the elements necessary for the verification of such winnings. In addition to this portable, stand-alone unit, there is a control system, outside the unit, which allows the payor entity to make necessary verifications before paying off the winnings.

Another object of the invention is to provide, inside the electronic unit itself, the drawing of the reference data to which the game data chosen by the player are compared. A further object of the invention is to allow simulation of one or several castings of dice, performing, inside the unit itself, a drawing of the game data, which are then compared to the predetermined reference data.

A very important consideration, inherent to such a gaming device, is the fight against fraud. In this regard, another object of the invention is to provide several securing and verification

levels, referring both to the origin of the portable unit and to the content of its information concerning, on the one hand, the "lose" or "win" aspects of the game, and, on the other hand, the value of the gain accumulated by the player, which may be quite significant.

Therefore, the invention provides an electronic system for implementing a game of chance, comprising:

a) a portable unit, comprising

- an input/output unit interface that can receive predetermined information authorizing the game, without which the unit cannot be used to play,
- a communication interface with the player,
- memory circuits capable of storing at least one set of reference data,
- unit processor, comprising:
- comparison media, which compare said reference data to the game data introduced by the player through the communication interface, whereby one of these two sets of data is a randomly generated value,
- media which can establish gain information, depending at least on the result of said comparison, and store this gain information in the memory, and
- unit encryption media, which, in response to a predetermined payment request received by the input/output unit interface, establish a first encrypted gain value based on said gain information, and deliver such first encrypted value to the unit interface, and

b) a control system, external to the unit, comprising

- an input/output system interface, which communicates with the input/output unit interface, and
- system processors, which,

. in the presence of a payment request from the player, read said gain information contained in the memory of the unit, and deliver said payment request information to the input/output system interface, and which include

. system encryption media, analog to the unit encryption media, which establish a second encrypted gain value based on said gain information being read, as well as comparison media that compare the two encrypted gain values; the actual payment of the winnings to the player is then subject at least to the matching of the two encrypted gain values.

Professionals know that the term "random" associated here to the generation of reference data or game data, is generally a mathematical concept, and that, in a practical embodiment of "random" generation, such generation is pseudo or quasi random, even though it is practically impossible to predict the data being generated. However, the term "random" is used here to reflect the practical impossibility, for a third party, to predict the game data or the reference data.

In one embodiment, system processors can transmit said predetermined game authorization information. On the other hand, in order to read gain information, in the presence of a payment request from the player, system processors can transmit a status request to the input/output system interface, in response to which unit processors deliver said gain information to the input/output unit interface.

In one embodiment, unit processors have a first set of random generators that can randomly generate said reference data from a predetermined series of values, while the communication interface has data entry media, allowing the player to choose his game data from the same predetermined series of values.

In order to assure the random drawing of the reference data, the first set of random generators conveniently include a game counter that operates from the start, prior to receiving said predetermined game authorization information; such counter can be stopped when a selected stop information is received, and can memorize the value it showed when stopped; this stop value determines said reference data.

The stop information preferably consists of said game authorization information.

In a variation, it is possible to design a game in which reference data are, for example, constants established in the rules of the game, the game data being randomly chosen by the player, in the way dice are cast. In such a variation, unit processors may include a secondary set of random generators, controlled by the action of the player, which can randomly deliver said game data, whereby the reference data are predetermined data stored in the memory.

To enhance security in the verification of the game information, the memory can store a first predetermined ancillary set of data, and the unit encryption media can generate the first encrypted gain value based on said gain information and said first set of ancillary data.

The first set of ancillary data is conveniently obtained based on a first ancillary encryption of at least a first set of information specific to the unit, such as its serial number, and is present in the memory before the receipt of the game authorization information.

In one embodiment, unit encryption media include:

- a pseudo-random gain encryption generator, which can be initialized at an initial value, and operate until it receives a stop command, in which case the first gain value is the value delivered by the pseudo-random gain encryption generator, upon receiving said stop command,

- a first logical circuit which can receive, as input variables, said gain information and at least part of the first ancillary data stored, apply a first logical predetermined function to these two input variables, and deliver a first corresponding output value, defining said initial value of the pseudo-random gain encryption generator, and

- an ancillary counter, which can count up or down, from an initial counter value to a final counter value; said command to stop the operation of the pseudo-random gain encryption generator is then delivered by the ancillary counter, when said final counter value is reached.

Unit encryption media also preferably include a second logical circuit that can receive as input variables a pseudo-random binary word, and at least a second part of the first ancillary data stored, apply a second logical predetermined function to these two input variables, and deliver a second corresponding output value, defining said initial counter value or said final counter value.

The system processors conveniently include system pseudo-random encryption media that can generate said pseudo-random binary word, which pseudo-random binary word accompanies said payment request information.

To verify the first encrypted gain value, system processors have a first set of ancillary encryption media which can perform said first ancillary encryption of said first specific information, in order to recalculate the value of the first ancillary data; on the other hand, system encryption media are analog to the unit encryption media, and can determine the second encrypted gain value based on the value of the first ancillary value recalculated, and on the pseudo-random binary word. This second encrypted gain value will then be compared to the first.

To verify again before payment, the memory conveniently can store a second predetermined ancillary value, and, in the presence of the player's payment request, system processors can verify the value of this second ancillary value, before delivering said payment request information to the unit. This second ancillary value can be a certificate, through an encryption algorithm with secret or public code, consisting of an identification specific to the control system, such as the serial number of a sale terminal.

To verify the origin of the unit, a convenient feature makes the memory capable of storing an identification of the unit, before receiving said game authorization information; the receipt of said game authorization information is then subject to the verification of this identification.

This identification data can result from an authentication encryption of a third item of information specific to the unit; this can be a certification of the serial number of the unit,

obtained from an encryption algorithm with secret or public code, using a key other than that reserved for the second ancillary data.

In this case, the system processors preferably contain authentication encryption media that can recalculate the identification data based on the third specific information, in order to verify the value of this third specific information read in the memory.

The serial number of the unit can be found in the memory of the unit. It can also be read by an appropriate reading device, such as an optical scanner, if the serial number appears in the form of a bar code on a label apposed on the unit.

In one embodiment, the memory has two levels, one containing the first ancillary data, the other containing first the identification data and then, after verifying the latter, the second ancillary data.

On the other hand, the memory can include a status counter that can contain status information representing the result of the game, as well as a payment counter that can contain payment information on a payment already made, or not yet made to the player.

In the presence of a payment request from the player, system processors can read, in addition, the content of the payment status counters, before delivering said payment request information to the unit.

The unit conveniently contains a power source, allowing the operation of at least some of these media, such as game counters and memory circuits, before receiving game authorization information.

The unit conveniently cannot play after a comparison between reference data and game data indicating a losing game and/or after an actual payment is made to the player.

The communication interface preferably includes media to give the player result information concerning the result of the comparison between game data and reference data, indicating whether he lost or won.

In one embodiment of the invention, the memory can store several reference data, and several game data which can be entered by the player.

These game data can be entered successively, each game datum entered being compared to a predetermined reference datum; a game datum cannot be entered by the communication interface unless the game data previously entered and the corresponding reference data match, whereby different gain information corresponds to each match.

Result information then conveniently displays the gain level corresponding to the gain information contained in the memory.

Memory circuits are preferably equipped with a gain counter that can successively contain predetermined binary gain words representing successive gain information, each binary word being different than the next and the preceding word by at least two bits. This allows having binary words sufficiently different between them, to properly differentiate the corresponding gain information, and especially to avoid errors caused, for example, by a mistaken reading or writing of a single bit. Equally, the status counter can conveniently contain successively predetermined status binary words representing successive status information, each binary word being different than the next and the preceding word by at least two bits.

When several game data must be entered by the player, especially successively, the first random generator preferably includes several game counters, each of which can contain reference data associated to game data entered by the player. Then, the receipt of said game authorization information may be set to stop the operation of all counters; then the multiple reference data are the multiple values found in the counters when receiving such game authorization information. In other words, the reference data is drawn once and for all, before the player enters the game data. However, it can be set so that a drawing takes place for each game datum entered. In this case, a single counter can be associated to all successive entries of game data by the player; when the player

enters game data, the counter is frozen at a value defining the reference value associated to such game data.

The control system conveniently includes a dialogue interface with the player, which can receive a payment request. This dialogue interface can be used for other purposes as well. Thus, in the presence of a request for verification of gain information from the player, the system processors can read the content of the gain counters, status counters, and payment counters, and communicate the results of this reading on the dialogue interface.

The control system can include at least one station, such as a terminal, and preferably several stations with analog structure, whereby game authorization and payment request information is delivered by the same station, or by two different stations.

To make another verification, especially when the gain is significant, the control system conveniently includes storage of a list of identification data of the winning and paid units and, in the presence of a payment request from the player, for a gain exceeding the predetermined gain value, system processors can verify whether the identification of the unit concerned is already found in said list.

Another object of the invention is a unit and a control system pertaining to such electronic device for a game of chance.

Other advantages and characteristics of the invention will appear from the examination of the detailed description of an embodiment, not limited thereto, and illustrated in drawings, as follows:

- figure 1 represents schematically a station and a unit according to the invention,
- figure 2 illustrates a network of stations,
- figures 3a, 3b, 3c represent in more detail the unit in figure 1,
- figure 4 represents a display screen of the unit,
- figures 5, 6 and 7 represent schematic synopses of the wired architecture of an ASIC component incorporated into the unit, and
- figures 8, 9, 10a, 10b, 10c represent operating layouts of

the device, and how the game is activated.

As illustrated in figure 1, the electronic gaming device has a portable unit 11 and a control system 12, external to the unit 12, and including an input/output system interface 17, including here two copper fields 17a and 17b that can communicate with the analog copper fields of an input/output interface of the unit 11, in order to exchange data by capacitive coupling.

In addition to this input/output interface 17, the control system 12 includes system processors 16, connected to this interface 17, as well as to a dialogue interface 13, with a user such as the seller or payor agent. This dialogue interface has a display screen 14, as well as a keyboard 15, for example for entering commands.

The system processors 16 are incorporated into an electronic card built around a micro-controller communicating with the interface 17 through an input/output register 88. As can be seen more in detail below, when the device is in operation, the system processors 16 have system encryption media 19, first and second ancillary encryption media 20 and 20b, authentication encryption media 21, as well as a system pseudo-random generator 22, that can generate a pseudo-random binary word whose meaning will be explained below. In reality, these various media are implemented logically in the micro-controller of the system processors.

In figure 1, the system processors 16, the input/output system interface 17, and the dialogue interface 13, are materially grouped in a station, such as a terminal. For this purpose, one can use a classic microcomputer, such as, for example, an IBM PC. In this case, the dialogue interface 13 will have the screen and the keyboard of the microcomputer. Then, one can use an additional electronic card, that can be introduced into the microcomputer, incorporating the system processors, as well as an extension constituting the interface 17.

Although, in general, the control system can be incorporated into a single station, it is planned to use a station network 12 (figure 2), all with analog structure. At least some of these

stations can be linked to storage units 23 that can store, as we will see more in detail below, a list of identifications of units having obtained a winning game, and having caused an actual payment to the player.

The unit 11 is sized, above all, so that it can be hand-held. On its front, (figure 3a), it has a key 24 which turns it on to activate at least some of its components, such as, for example, the display screen 28. On the other hand, this example of embodiment contains three game keys 25, 26 and 27, bearing three figures (1, 2 and 3), representing three game data among which the player can choose.

On the back, (figure 3c), there is a label on which there appears, for instance, in bar code, the serial number NS of the unit. Here, this serial number constitutes a unique identification, specific to the unit.

Figure 3b schematically illustrates an internal view of the unit 11. It shows the electronic prints 21, 32, 33 and 34 of the keys 24, 25, 26 and 27. Two copper fields 29 and 30, which are part of an input/output unit interface, can communicate with the two matching copper fields 17a and 17b of a station 12. Autonomous power sources 35 and 36, such as batteries, assure the autonomy of the portable unit and, as we will see below, permanently supply power to certain components of the unit.

While the three game keys 25, 26, 27, and the display screen 28 form a communication interface with the player, an essential element of the invention is here a specific integrated wired circuit (ASIC: Application Specific Integrated Circuit) bearing reference 37, and, as we will see in more detail below, comprising the unit processors, as well as the memory circuits. This ASIC is linked by a connection network 38 to the game keys, power sources, as well as the display screen 28. Of course, instead of an ASIC component, a micro-controller could have been used, incorporating in the software at least some of the functions of the unit described below. However, the use of an ASIC reduces manufacturing costs, and makes the device under the invention more secure against

fraud. Indeed, it is more difficult for a defrauder to access and understand the architecture of a wiring diagram specifically built for an application, and incorporated into an ASIC, than to obtain the instructions of a software incorporated in the memory of a micro-controller program.

Figure 4 shows a display screen 28, such as it may appear to the player in the specific application of the game described in this example. At the bottom of the display screen there are two spaces GA and FI, where the messages "GAGNE" /win/ and "FIN" /end/ may appear, depending on whether the player won or lost in his game of chance. On the two sides of the screen there respectively appear two columns with spaces numbered 1, 2, 3, 4, 5 and 6, 7, 8, 9, 10. These spaces bear references NG1-NG10, and correspond to successive gain levels reached by the player during the game. In the middle of the display screen there are spaces for three arrows F, respectively positioned across from circular spaces N1, N2 and N3, inside which there appear the three figures 1, 2 and 3. As we will see below, one of these arrows F will mark the choice of the player after having pressed one of the game keys 25 to 27, while one of the spaces N1, N2 or N3 will mark the reference data randomly drawn by the unit itself.

Figure 5 shows schematically part of the elements contained in the component 37. First, there is an input/output serial/ parallel register 39, which is part of the input/output unit interface, and linked to the two copper fields 29a and 30. This register 39 is connected to a decoding circuit 40 which can decode the various items of information received by the register 39 (input/output, writing, reading). This decoding circuit 40 is linked to a formatting circuit 51, connected first to a status counter 48, such as a non-linear counter, which can contain status information representing the "loss" or "gain" result of the game, secondly to a counter 49, which can contain information on a payment actually made to the player, and thirdly, to a so-called gain counter 50, such as a non-linear counter, which can contain gain information depending on the result of the game. In response to a status

request, the formatting circuit can deliver to the input/output register 39 the contents C1, C2, C3 of the three aforementioned counters 48, 49 and 50.

The output of the gain counter 50 is also linked to the input of the first logical circuit 47, whose other input is linked to a first live memory M1. The output of the first logical circuit is linked to a pseudo-random generator called gain encryption generator 46, such as a polynomial counter or a cyclic generator, also controlled by an ancillary counter 45 which receives at its input the output of the second logical circuit 44, the two inputs of which are respectively linked to the memory M1 and to the input/output register 39. The output of the gain encryption generator 46 is linked to the register 39.

Also included are logical control media 41 for all these elements, sequenced by a clock signal CLK with a frequency, for example, of 500 kHz, delivered by an oscillator 43.

Another live memory M2, linked to the input/output register 39, is part, along with M1, of the memory of the unit.

Figures 6 and 7 illustrate in more detail the first random generation media capable of generating the reference data which will be compared to the data entered by the player.

Figure 6 represents an embodiment applicable to drawing of lots, made once for several successive reference data (ten, for example), corresponding respectively to potential successive game data entries made by the player.

A logical part ET 52 receives at the input the clock signal CLK, as well as game authorization information DV, the meaning of which will be explained in more detail later. The output of this logical port 52 is linked to the first module counter 2 (53-1) of a range of ten counters 53-1 to 53-10, connected in cascade, whose output is respectively linked to the ten inputs of a multiplexer 54, whose output is linked to the first input of a comparator 55. Each comparator can therefore display a content corresponding to one of the three figures 1, 2 and 3. This multiplexer 54 is controlled, concerning the choice of its input path, by the output

of the gain counter 50. The other input of the comparator 55 receives the value VJ /"valeur de jeu" = game value/ of the game data entered by the player. The output of this comparator is linked to the status counter 58 and to the gain counter 50.

As we will see below, figure 7 illustrates a more particularly adapted embodiment, either for successive drawings associated respectively to the successive entries of game data made by the player, or to the random generation of game data which will be analogous, for example, to the casting of dice by the player. In this latter case, the reference data which will be compared to the randomly generated game data may be a constant stored in the memory of the unit. In this embodiment, the logical port 52 receives, instead of the game authorization information DV, the signal ACI of game data entered by the player on the communication interface. In this case, there is only one counter 53, linked to this logical port 52, the output of which is linked to the first input of the comparator 55.

Now we are going to describe more in detail the operation of the device under the invention, referring more particularly to figures 8 to 10c.

During manufacture at the factory (stage 56), a first set of ancillary data IC1 is stored in the memory M1, while a set of authentication data IC2 is stored in the memory M2 (stage 57 and stage 58). The first set of ancillary data IC1 constitutes a first securization, which will be used for actual payment of winnings to the player. In general, it results from a first ancillary encryption of information specific to the unit. More precisely, this is, for example, encrypted information obtained from a serial number NS of the unit through an encryption algorithm of the secret code type, such as that known by the abbreviation DES (Data Encryption Standard), and using a first secret code for this purpose. It would also be possible to use an encryption algorithm with public code, such as that known by the abbreviation RSA (Rivest Shamir Adelman).

The set of identification data IC2 also consists of

authentication encryption of information specific to the unit. Concretely, this is an encryption of the serial number of the unit, based on a secret (or possibly public) code algorithm, with a different code than that used for the information IC1. This data set IC2 is, in fact, a certificate of the serial number NS.

In order to preserve the content of the live memories M1 and M2, the unit will be permanently fed by its power sources installed at the factory. Therefore, said counters 53-1 to 53-10 operate from the manufacture stage of the unit at the factory.

However, at this stage, the unit is unable to play, or locked. In other words, the unit processors are inactive, and a player who obtains such unit would not be able to enter game data using the keys 25-27.

When released from the factory, the unit is stored in a sales facility equipped with a control station 12. When such a unit is sold to a player, it is first validated (stage 59). With the unit set on the unit interface 17, the unit processors 16 read the content of the memory M2, and the authentication encryption media 21 recalculate the authentication data IC2, based on the serial number NS and the value of the secret code used (also present in the memory of the station). For this purpose, the unit processors can know the serial number NS of the unit, either because it is directly stored in the memory M2 of the unit, or by optically reading, with a proper reader, the bar code located on the back of the unit. The matching of the authentication data with the data present in the memory M2 before this validation stage 59 allows making a first verification concerning the origin of the unit, and thus assuring that, a priori, the unit is authentic.

After completing this verification of origin, the second ancillary encryption media 20b of the unit processors determine a second set of ancillary encrypted data IC3, also based on information specific to the selling station, and a secret (or possibly public) code encryption algorithm, using a third code, different than the first two. Practically, the second ancillary encryption media use as unit-specific information its serial

number, the date of the sale, as well as a sequence number of the sale on that date, and determine the encrypted certificate of this unit-specific information. Then, the unit processors store this station-specific information, as well as the certificate IC3, in the memory M2.

The match between the authentication data set IC2, stored in the memory M2, and the recalculated data, also leads to the issuance of the game authorization information DV by the station processor; on the one hand, this will activate the unit processor in order to make the unit ready to play and, on the other hand, it will stop the operation of the game counters 53-1 to 53-10. This game authorization information, as well as the status request, are actually special commands issued by the station, at the receipt of which the unit processors perform predetermined operations. It is noteworthy that, in this embodiment, the set of reference data is then the set of values shown by the counters 53-1 to 53-10 when receiving the game authorization information. These reference data will be saved in the counters 53-1 to 53-10 for comparison with game data. The drawing of all reference data was therefore done once only. On the other hand, the quick pace of the operation of the counters, as well as the random character of the instant the counters are started at the factory, and the instant the information DV is received, contribute to the "random" character of the reference data generated.

Of course, in the variation illustrated in figure 7, with successive drawings of reference data, the receipt of the game authorization information DV has only the effect of activating the unit processors, and of unlocking the unit to make it ready to play.

The player now has a unit which is ready to play.

The game stage proper 60, here corresponding to a particular example of game, is illustrated in more detail in figure 9. When the unit is activated (stage 61) by pressing the key 24, the screen 28 displays (stage 62) the figures 1, 2 and 3 in the spaces N1, N2 and N3, as well as the previous gain level. If the player has never

before played with this unit, there is, of course, no display of the previous gain level.

In stage 63, the player chooses a figure and presses the corresponding key 25-27, thus entering his game data. The arrow F, pointing to the spaces N1, N2 or N3, according to the digit chosen by the player, is displayed, and unit processors activate a visual animation software, commonly called "chain" by professionals, which causes the figures 1, 2 and 3 to spin on the display screen 28, simulating the movement of a roulette in a roulette game. Then, the "chain" simulates the deceleration of the roulette, and the figure corresponding to the reference data contained in the first game counter 53-1 is displayed in the corresponding location on the display screen 28 (stages 64, 65).

If the figure is displayed facing the arrow F which marked the game data chosen by the player (stage 67), the player wins. In this case, the word "GAGNE" /wins/ is displayed in the GA location, and the gain level 1 is displayed in the NG1 location. Otherwise (stage 66), i.e. if the figure corresponding to the reference data is not displayed facing the arrow F, the player lost, and the word "FIN" /end/ is displayed in the FI location. In this case, the unit processor locks (stage 68) the communication interface with the player, in the sense that the latter can no longer enter game data with the keys 25-27. In other words, the unit is again made unable to play, and can be thrown out, for example.

If he wins, the player has two possibilities. He either decides to stop playing and request payment of his winnings, by going to the station 12, or he decides to try his chance once more, by choosing again a game data set which he enters by using the keys 24-27. Then the game repeats stages 63 to 66 or 67. In the embodiment illustrated in figure 6, the content of the gain counter allows selecting the input path of the multiplexer 54, since this gain counter contains different gain information for each winning attempt of the player. Thus, in this case, on the second attempt, the second counter 53-2 of the chain will be selected, and its content, corresponding to the second reference data set, will be

compared to the game data entered by the player. The player can thus try his chance ten times one after the other, hoping to reach the gain level 10. With each winning attempt, his current gain level is displayed, and is higher than the preceding gain level. On the contrary, if during this sequence of events, an attempt loses, the unit can no longer play, and the preceding gain level remains displayed. Of course, the player can make a further attempt only if he won on the previous attempt, i.e. if the reference data in his preceding attempt matched the game data he entered at that time.

In the embodiment illustrated in figure 7, the ten reference sets of data corresponding to the ten gain levels are not predetermined in advance. The counter 53 works until a key 24-27 is pressed by the player, marking his choice of game data. This action ACJ /activating game choice/ then blocks the counter 53 on a value defining the randomly generated reference value, associated to the game data entered by the player during his attempt. After displaying a possible winning result, the counter 52 continues to work, and will again freeze on another value, if the player enters another game value.

The variation in figure 7 is also compatible with another type of game, consisting, this time, of comparing the constant predetermined reference values stored in memory, to game data entered randomly by the player. This simulates a casting of dice by the player. In this case, the receipt of the signal in ACJ, caused by the player's pressing an appropriate key on the unit, causes the counter 53 to stop, marking the random generation of the game data, which will be then compared to the reference value (here also indicated by VJ) stored in memory.

If a player who won and reached a certain gain level decides to stop playing and to request payment of his winnings, he makes a payment request 69 to a station 12, which then begins an in-depth verification stage 70. We must note, at this point, that the player can request such payment from the same station that sold him his unit, or from a similar station.

We now refer more particularly to figures 10a to 10c, in order

to describe this verification stage.

This stage begins with a visual verification 71 by the agent in charge of making payments. This visual verification consists of verifying the display of the word "GAGNE," as well as the display of a gain level. If no error 72 appears, the unit is then placed on the input/output interface 17 of the station, and the system processors deliver a status request (stage 73) through the unit processors. Upon receipt 74 of this status request ST1, the unit processors deliver to the input/output register 39 the respective contents C1, C2, C3 of the counters 48, 49 and 50, as well as the content of the memory M2. The respective contents C1, C2, C3 are then displayed in "clear" on the screen 14 of the dialogue interface of the station (stage 78). This constitutes another visual verification which, however, is not sufficient proof for actual payment of the winnings to the player, as explained below.

A verification stage 81 then begins, consisting of verifying the value of the second ancillary data IC3 contained in the memory M2. For this purpose, the second ancillary encryption media of the station system processors read the station-specific information (serial number of the station, date of sale and sequence order) in the memory M2, and recalculate the certificate IC3 of this specific information, in order to compare it to that contained in the memory M2.

A non-matching of these two data sets IC3 also leads to an error 82 which can interrupt the payment process. Otherwise, the system processors compare the gain information from the gain counter 50 to a predetermined gain value GS. If the gain is higher than this value GS, the system processors verify whether the identification of the unit in question, i.e. its serial number, is not already on a list of winning unit identifications which were already paid. If this is the case, there would also be an error 85, which interrupts the payment process. If the station 12 is not linked to the storage media 23 of this list, the player is asked to go to a station linked to this list. Of course, the player can be asked to change stations immediately after the visual verification

71.

If the gain is lower than the GS value, or if the gain is higher than the GS value and the unit is not on the winning list, the system processors issue (stage 86) payment request information (IDP) accompanied by an aleatory binary word MBA. Upon receipt 87 of the information IDP and the binary word MBA through the unit input/output interface, the encryption media (44, 45, 46 and 47) of the unit can generate a first encrypted gain value VF1, based on the gain information contained in the gain counter 50 and the first ancillary data set IC1 contained in the memory M1 (stages 88-92).

For this purpose, the pseudo-random gain encryption generator 46 can be initialized at an initial value, and operate until it receives a stop command. The first encrypted gain value VF1 is then the value delivered by the pseudo-random gain encryption generator 46 when receiving such stop command.

The first logical circuit 47 receives, as input variable, the gain information contained in the gain counter 50, and part of the first ancillary data set IC1 contained in the memory M1. This first circuit 47 then applies a first predetermined logical function, for example based on an exclusive OU /or/, to these two input variables, and delivers a first corresponding output value, which defines the initial value of the pseudo-random gain encryption generator 46.

The ancillary counter 45 can count up or down from an initial counter value to a final counter value. The command to stop the operation of the pseudo-random gain encryption generator is then delivered by the ancillary counter 45, when said final counter value is received.

The second logical circuit 44 is used here to define the initial counter value, or the final counter value, depending on whether the counter counts up or down.

This second logical circuit receives, as input variable, the pseudo-random binary word MBA and a second part of the first stored ancillary data set IC1. A second predetermined logical function, preferably different than the first. is then applied to these two

input variables, and the second logical circuit 44 delivers a second output value, which defines the initial counter value or the final counter value.

Thus, the polynomial counter (for example) 46, is initialized at an initial value depending on the encrypted content of the memory M1 and on the gain information contained in the gain counter 50. This counter operates then until the ancillary counter 45 stops, the number of repetitions of the latter being defined pseudo-randomly with the help of the binary word MBA. When the counter 46 stops, its content, which defines the first encrypted gain value VF1, is delivered to the system processors of the station through the intermediary input/output register 39 (stages 93, 94).

The actual payment of the winnings to the player will take place only if this first encrypted gain value VF1, delivered by the unit, is identical to a second encrypted gain value VF2, established by the system encryption media 19 of the station. For this purpose, the first ancillary encryption media 20a of the station recalculate the first ancillary encrypted data IC1 based on the serial number of the unit and the corresponding secret code. This serial number can be stored in the memory M1, or read optically by an optical scanner. Starting from there, the system encryption media, which are similar to the unit encryption media (i.e. logical circuits and counters analogous to logical circuits 44, 47 and counters 45 and 46), calculate the second encrypted gain value, similarly to that used for the calculation of the first encrypted gain value, based on the information IC1 recalculated by the first ancillary encryption media, and the pseudo-random binary word MBA, which is known to the station because it is generated by the pseudo-random generation media of the system 22.

If the two sets of data do not match, a new error appears and interrupts the payment process. On the contrary, if they match, the payment 99 of the winnings is made to the player, the unit is locked (stage 101), the counter 49 is loaded with information concerning the payment made to the player, and the serial number of

this winning unit is stored (stage 100), either at the station itself, or in the storage media 23, especially in the event of a gain higher than the value GS.

The fact that the actual payment of the winnings to the player is subject to the matching of the two encrypted gain values VF1 and VF2 guarantees the payor entity against fraud, especially that caused by counterfeit units containing microprocessors programmed to simulate fake gain information values.

Although the other verification stages (status request. verification of data IC2 and IC3) are not indispensable, they conveniently contribute to increase securization against fraud. On the other hand, the professional would have understood that only the content of the counters 48, 49 and 50 have value of proof for the payor entity, and that the display of their content on the screen 14 or 28 is merely a visual indication. Thus, and also in order to increase securization, the gain counter 50 is conveniently designed to contain successively predetermined binary gain words representing successive gain information that the player could obtain if he successively won at each attempt. Each binary word is then different than the preceding and following words found on the list, by at least two bits. Such a precaution complicates further the task of a defrauder who would seek to modify the content of the gain counter, because he would have to modify two bits at a time, rather than one.

The same precaution can be conveniently used for the status counter 48, with a second predetermined list of binary words differing from each other by at least two bits. In addition, this brings double securization for the verification of the gain level obtained and the losing or winning status of the game at each attempt.

Finally, a player may wish to purchase a unit from a third party in order to continue the game. In this case, it is especially beneficial that the buyer can verify, in particular, the content of the gain counter. Thus, in the presence of a verification request concerning gain information coming from the buyer player, the

system processors can read the contents of the gain, status and payment counters, and communicate the results of such reading on the screen 14 of the dialogue interface. Of course, in this case, the payment request information IDP is not delivered to the unit.

CLAIMS

1. Electronic device implementing a game of chance, comprising

a) a portable unit (11) containing

- an input/output unit interface (39, 29, 30) that can receive predetermined game authorization information without which the unit cannot play,

- a communication interface (24, 25, 26, 27, 28) with the player,

- memory circuits (M1, M2, 53-1,... 53-10, 48, 49, 50) that can store at least one reference data set,

- unit processor, containing

. comparison media (55) that can compare said reference data with game data entered by the player using the communication interface, one of these two data sets being a randomly generated value,

. media (50) that can establish gain information depending at least on the result of said comparison, and store such gain information in the memory (50), and

. unit encryption media (44-47) that, in response to predetermined payment request information (IDP) received by the input/output unit interface, can establish a first encrypted gain value (VF1) based on said game information, and deliver this first encrypted gain value to the unit interface, and

b) a control system (12), external to the unit (11), comprising

- an input/output system interface (17) that can communicate with the input/output unit interface, and

- system processors (16), that can,

. in the presence of a payment request from the player, read said gain information contained in the unit memory, and deliver said payment request information (IDP) to the input/output system interface, and comprise

. system encryption media (19), similar to the unit encryption media, which can establish a second encrypted gain value (VF2)

based on said gain information read, as well as comparison media that can compare the two encrypted gain values,

whereby the actual payment of the winnings to the player is subject at least to the matching of the two encrypted gain values.

2. Device according to claim 1, characterized by the fact that the system processors can transmit said predetermined game authorization information (DV).

3. Device according to claim 1 or 2, characterized by the fact that the unit processors include first random generation media (53-1,... 53-10) that can randomly generate said reference data from a predetermined series of values, while the communication interface has data entering media (25-27), allowing the player to choose his game data among the same predetermined series of values.

4. Device according to claim 3, characterized by the fact that the first random generation media have at least one game counter (53-1... 53-10) that operates from an initial instant preceding the receipt of said predetermined game authorization information (DV), this counter being liable to the stopped when receiving a chosen stop command (DV) and to save the value it shows when its operation stops, whereby said stop value defines said reference value.

5. Device according to claim 4, characterized by the fact that the stop information constitutes said game authorization information (DV).

6. Device according to claim 1 or 2, characterized by the fact that the unit processors include second random generation media (53), controlled by the action of the player, that can randomly deliver said game data, whereby the set of reference data is a set of data previously stored in the memory.

7. Device according to one of the preceding claims, characterized by the fact that the memory circuits (M1) can store a first set of predetermined ancillary data (IC1),
and by the fact that unit encryption media (44-47) can generate the first encrypted gain value (VF1) based on said gain information and said first set of ancillary data (IC1).

8. Device according to claim 7, characterized by the fact that

the first set of ancillary data is obtained based on a first ancillary encryption of at least a first item of information (NS) specific for the unit, and is present in memory (M1) before the receipt of the game authorization information (DV).

9. Device according to claim 7 or 8, characterized by the fact that the unit encryption media include:

- a pseudo-random gain encryption generator (46) that can be initialized at an initial value, and operate until it receives a stop command, in which case the first encrypted gain value (VF1) is the value delivered by the pseudo-random gain encryption generator, when receiving said stop command,
  - a first logical circuit (47) which can receive, as input variables, said gain information and at least part of the first ancillary data stored (IC1), apply a first logical predetermined function to these two input variables, and deliver a first corresponding output value, defining said initial value of the pseudo-random gain encryption generator, and
  - an ancillary counter (45), which can count up or down, from an initial counter value to a final counter value; said command to stop the operation of the pseudo-random gain encryption generator (46) is then delivered by the ancillary counter, when reaching said final counter value.

10. Device according to claim 9, characterized by the fact that the unit encryption media include a second logical circuit (44), which can receive, as input variable, the pseudo-random binary word (MBA) and at least a second part of the first stored set of ancillary data (IC1), apply a second predetermined logical function to these two input variables, and deliver a second corresponding output value, which defines said initial counter value or the final counter value.

11. Device according to one of the claims 7 to 9, characterized by the fact that the system processors have a system pseudo-random generator (22), that can generate a pseudo-random

binary word which accompanies said payment request information (IDP).

12. Device according to claim 11, combined with claim 8, characterized by the fact that system processors include the first ancillary encryption media (20a), which can perform the first ancillary encryption of the first specific information (NS) in order to recalculate the value of the first ancillary data (IC1), by the fact that system encryption media are similar to the unit encryption media
and by the fact that the system encryption media can determine the second encrypted gain value (VF2) based on the value of the first recalculated ancillary data (IC1) and the pseudo-random binary word (MBA).

13. Device according to one of the preceding claims, characterized by the fact that memory circuits can store a second set of predetermined ancillary data (IC3), and that, in the presence of a request for payment by the player, the system-encryption media can process a verification (81) of the value of this second set of ancillary data before delivering said payment request information to the unit.

14. Device according to claim 13, characterized by the fact that the system processors have a second set of ancillary encryption media (20b), which can perform a second ancillary encryption of a second information specific for the control system, in order to determine the second set of ancillary data (IC3), at the latest when receiving said game authorization information from the unit,
by the fact that the system processors can store said second specific information and the second set of ancillary data (IC3) in the memory (M2),
by the fact that the second ancillary encryption media can read the second specific information and the second set of ancillary data in the memory of the unit, and compare the value of the second set of ancillary data read to that recalculated by the second ancillary encryption media based on the second specific information read.

15. Device according to one of the preceding claims, characterized by the fact that the memory is able to store unit authentication data (IC2) before receiving said game authorization information,

and by the fact that the receipt of said game authorization information depends on the verification of these authentication data.

16. Device according to claim 15, characterized by the fact that the authentication data arise from the encryption of the authentication of a third information specific to the unit (NS),

by the fact that the system processors have authentication encryption media (21) that can recalculate the authentication data (IC2) based on the third specific information, in order to verify the value of this third specific information read in the memory (M2).

17. Device according to one of the claims 8 to 16, characterized by the fact that the first and second ancillary encryption, as well as the authentication encryption, have code encryption algorithms, and by the fact that the second ancillary data and the authentication data are encrypted certificates of the second and third specific information.

18. Device according to one of the claims 8 to 17, characterized by the fact that the first and third specific information have an identification specific to the unit, such as the serial number of the unit, and by the fact that the system processors have media that can read the serial number.

19. Device according to one of the preceding claims, characterized by the fact that the memory has two memory circuits (M1, M2), one of which contains the first ancillary data, and the other the first set of authentication data (IC2) and then, after verifying the latter, the second set of ancillary data (IC3).

20. Device according to one of the preceding claims, characterized by the fact that the memory has a status counter (48) which can contain status information representing the result of the game, as well as a payment counter (49), which can contain

information on a payment actually made to the player, or not yet made to the player,

by the fact that, in the presence of a payment request from the player, the system processors can also read the content of the status and payment counters, before delivering said payment request information to the unit.

21. Device according to one of the preceding claims, characterized by the fact that it has power supply media (35, 36), allowing at least certain unit features to function before receiving game authorization information.

22. Device according to one of the preceding claims, characterized by the fact that the unit cannot play after a comparison between reference data and game data showing a losing game and/or after an actual payment is made to the player.

23. Device according to one of the preceding claims, characterized by the fact that the communication interface has media (28) for returning to the player result information concerning the result of the comparison between game and reference data, indicating to him whether he lost or won.

24. Device according to one of the preceding claims, characterized by the fact that the memory circuits can store several reference data, and

by the fact that several game data can be entered by the player.

25. Device according to claim 24, characterized by the fact that game data are entered successively, each game datum entered being compared to a predetermined reference datum,

and by the fact that a game datum cannot be entered through the communication interface unless there is a match between the previously entered game datum and the corresponding reference datum,

and by the fact that to each match corresponds a different gain information item (NG1,... NG10).

26. Device according to claims 23 and 25, characterized by the fact that the result information comprises the display of gain

level information corresponding to the gain information contained in the memory.

27. Device according to one of the claims 24 to 26, characterized by the fact that the memory has a gain counter (50) that can successively contain predetermined binary gain words representing successive gain information, each binary word differing from the following and preceding word by at least two bits.

28. Device according to one of the claims 24 to 27, in combination with claim 20, characterized by the fact that the status counter (48) can contain successively predetermined status binary words representing successive gain information, each binary word differing from the following and preceding word by at least two bits.

29. Device according to one of the preceding claims, in combination with claims 4 and 24, characterized by the fact that the first random generation media have several game counters (53-1,... 53-10), each counter being capable of containing a reference datum, and being associated to the entering of a game datum by the player.

30. Device according to claim 29, characterized by the fact that the receipt of said game authorization information (DV) stops the operation of the counters, in which case the various reference data are the various values shown by the counters when they received this game authorization information.

31. Device according to one of the claims 1 to 28, in combination with claims 4 and 25, characterized by the fact that the counter is associated with every successive entering of game data by the player, and by the fact that the entering of a game datum by the player corresponds to a value defining the reference value associated to this game datum.

32. Device according to one of the preceding claims, characterized by the fact that the control system has a dialogue interface (14, 15) that can receive said payment request from the player.

33. Device according to claim 32, characterized by the fact that, in the presence of a request for verification of gain information from the player, the system processors can read the content of the gain counters, status counters, and payment counters, and communicate the results of this reading on the dialogue interface.

34. Device according to one of the preceding claims, characterized by the fact that, in the presence of a payment request from the player, the system processors can transmit to the input/output system interface a status request (STI), in response to which the unit processors deliver said gain information to the input/output unit interface.

35. Device according to one of the preceding claims, characterized by the fact that the control system has at least one station, such as a terminal.

36. Device according to claims 14 and 35, characterized by the fact that the second specific information has the serial number of the station, the date of sale of the unit to the player, and the sequence number of that sale on that date.

37. Device according to claim 35 or 36, characterized by the fact that the control system has several stations with analog structure, whereby game authorization information and payment request information can be delivered by the same station or by two different stations.

38. Device according to claims 35 to 37, characterized by the fact that each unit has a unique identification, by the fact that the control system has storage capacity (23) for a series of identifications of winning and paid units,
by the fact that, in the presence of a payment request from the player and corresponding to a gain higher than a predetermined gain value, system processors can verify whether the identification of the unit concerned is already on said list.

39. Device according to the preceding claims, characterized by the fact that the unit has a wired integrated circuit (37), containing the unit processors and the memory of the unit.

40. Unit pertaining to the device according to one of the claims 1 to 39.

41. Control system pertaining to the device according to one of the claims 1 to 39.

TCA Translation

Fig. 1

/Diagram/

Fig. 2

/Diagram/

Fig. 3c

/Diagram/

Fig. 3b

/Diagram/

Fig. 3a

/Diagram/

Fig. 4

/Diagram/

TCA Translation

Fig. 5

/Diagram/

Translated by:
TCA-Translation Co. of America
10 West 37th Street
New York, N.Y. 10018

(212) 560-7054

Fig. 6

/Diagram/

"vers" = towards

Fig. 7

/Diagram/
"vers" = towards

Fig. 8

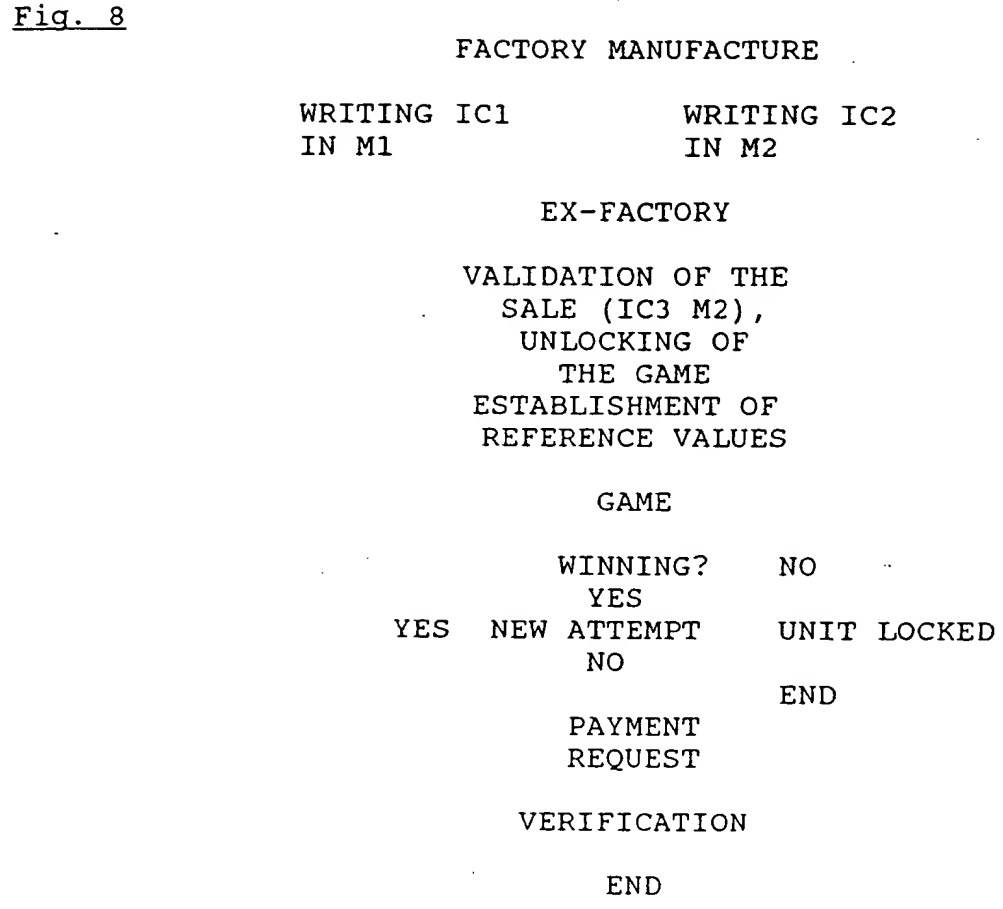

FACTORY MANUFACTURE
WRITING IC1 IN M1
WRITING IC2 IN M2
EX-FACTORY
VALIDATION OF THE SALE (IC3 M2), UNLOCKING OF THE GAME ESTABLISHMENT OF REFERENCE VALUES
GAME
WINNING?
YES
NO
YES
NEW ATTEMPT
NO
UNIT LOCKED
END
PAYMENT REQUEST
VERIFICATION
END

Fig. 9

TURNING ON

DISPLAY FIGURES AND PREVIOUS GAIN LEVEL

CHOICE OF FIGURE AND PRESSING OF A KEY

POSITIONING OF ARROW AND FIGURE ROTATION

NO

DISPLAY FIGURE ACROSS FROM THE ARROW ?

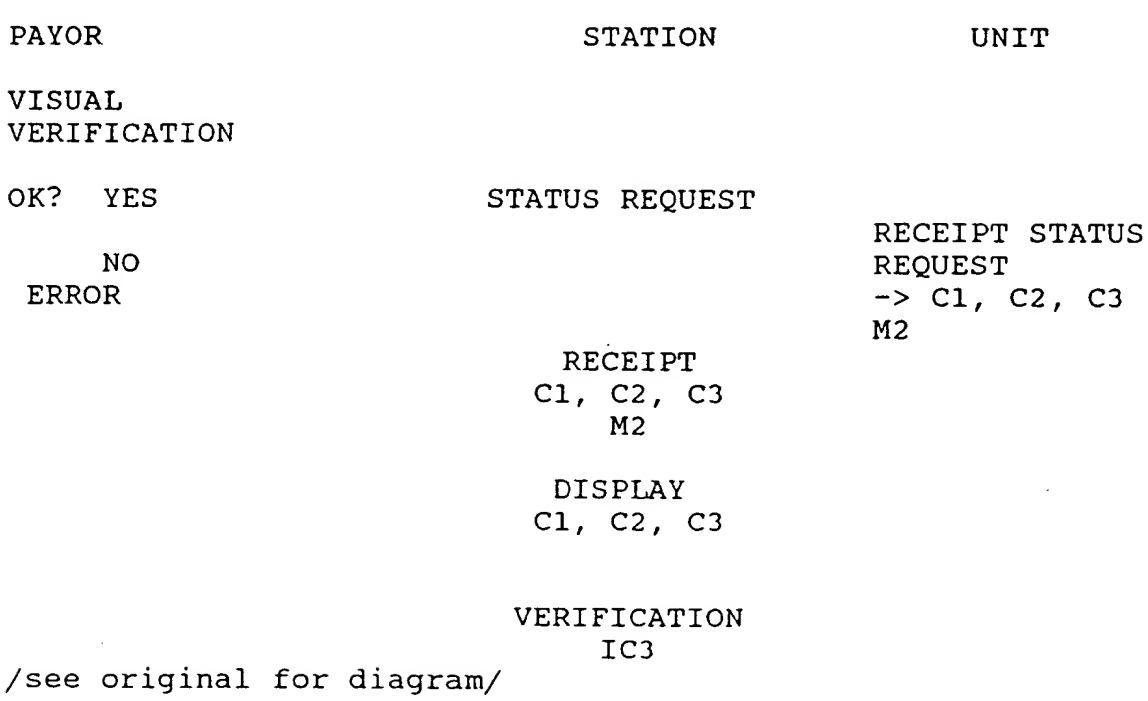
YES

LOSS; DISPLAY "END" + PREVIOUS GAIN LEVEL

DISPLAY "WIN" + CURRENT GAIN LEVEL

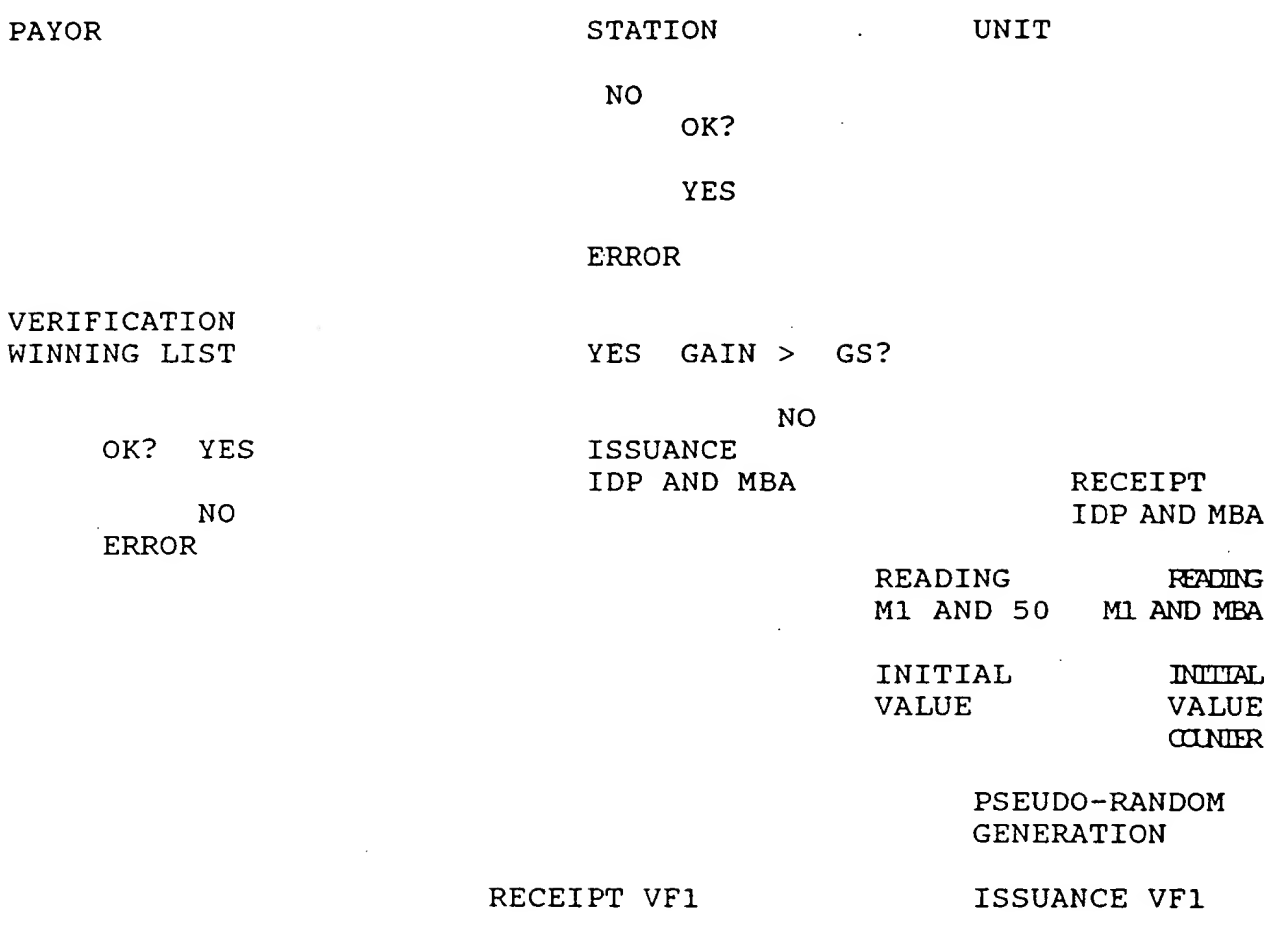
/see original for diagram/

Fig. 10a



/see original for diagram/

Fig. 10b



/see original for diagram/

TCA Translation

Fig. 10c

PAYOR STATION UNIT

CALCULATION
CONTENT M1

CALCULATION VF2

VF1 =? VF2

NO YES
ERROR

PAYMENT

STORAGE UNIT LOCKED

END END

/see original for diagram/

TCA Translation

42 2697653

REPUBLIC OF FRANCE

NATIONAL INSTITUTE OF
INDUSTRIAL PROPERTY

National registration No.
FR 9213239
FA 478979

RESEARCH REPORT
issued based on the latest claims
registered before the beginning of the research

DOCUMENTS DEEMED PERTINENT		Claims concerned of the application examined
Category	Document quotation with indication of pertinent parts, if necessary	
A	WO-A-8 902 139 (AMERICAN TELEPHONE TELEGRAPH COMPANY) * summarized* * page 3, line 13 - page 5, line 12 * ---	1
A	WO-A-9 106 931 (RAHA) * summarized* ---	1
A	EP-A-O 450 520 (GANOT) *column 2, line 43 - column 3, line 2 * * column 4, line 54 - column 5, line 34* ---	

TECHNICAL FIELDS OF RESEARCH (Int'l Cl.5)
GO7F

Date of research completion
JULY 13, 1993

/Illegible/
TACCOEN J-F.P.L.

CATEGORY OF DOCUMENTS CITED

X: Especially pertinent by itself
Y: Especially pertinent along with another document of the same category
A: Pertinent in opposition with one /illegible/ general technical claim

TCA Translation

O: Non-written disclosure

P: Intercalary document

T: Theory in principle underlying the invention

E: Patent document dated prior to the application date, and which was not published other than on that application date or later

C: Cited in application

L: Cited for other reasons

/illegible/: Member of the same family, corresponding document